UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

BMG RIGHTS MANAGEMENT (US) LLC, and ROUND HILL MUSIC LP, Plaintiff, v. COX ENTERPRISES, INC., COX COMMUNICATIONS, INC., and COXCOM, LLC, Defendants.	Case No. 1:14-cv-1611 (LOG/JFA)

COX'S BRIEF IN OPPOSITION TO PLAINTIFFS' MOTION FOR EVIDENTIARY SANCTIONS

REDACTED NON-CONFIDENTIAL VERSION

TABLE OF CONTENTS

Page

INTRODUCTION

In their motion for evidentiary sanctions (Dkt. 340), Plaintiffs ask the Court to sanction Cox for its routine purging of transitory dynamic host configuration protocol (DHCP) data that served no business purpose and posed consumer privacy risks. Cox is not guilty of spoliation, as explained in detail below. But the Court need not reach the spoliation issues, because Plaintiffs' motion has two fundamental and fatal flaws.

First, Plaintiffs never asked for the DHCP logs in discovery. The Court will note that Plaintiffs' motion does not reference any discovery request to which Cox has failed to respond. Plaintiffs *did* seek personally identifiable information (PII) for Cox subscribers potentially implicated by Plaintiffs' infringement claims (more on that below). But despite knowing, since March 2015 (over *four months* before the close of discovery), that Cox had DHCP logs extending back to at least the filing of the lawsuit, ***Plaintiffs never asked for that data***. This entire motion is sleight-of-hand: Plaintiffs seek extraordinary and disproportionate sanctions for alleged spoliation of evidence they never requested.

Second, even if Plaintiffs had sought and received the DHCP logs in discovery, that data would be useless. The DHCP logs are merely a method for connecting a particular IP address to a particular cable modem. The Cox Abuse Tracking System (CATS), or a Cox customer service representative, must then associate that modem with a particular Cox subscriber's account using other data. Consequently, without that connective information, the DHCP data would tell Plaintiffs literally nothing. What Plaintiffs really wanted, and what they sought in discovery, was not DHCP data but PII for Cox subscribers. Cox refused to produce that PII because (i) the Cable Privacy Act precluded Cox from doing so, (ii) the request invaded the privacy of Cox's subscribers, and (iii) the information was irrelevant because Plaintiffs have consistently

disavowed any intention or need to prove infringement by any particular Cox subscriber. Plaintiffs moved to compel production of Cox subscribers' PII and the Court largely denied that motion. The Court ordered Cox to produce PII only for subscribers historically associated with a "sampling" of 250 IP addresses identified by Plaintiffs. Cox was able to produce PII for more than half of those IP addresses but, as Cox explains later in this brief, Plaintiffs did essentially *nothing* with that information after fighting so hard to get it. In any event, the notion that the DHCP logs are a trove of information Plaintiffs could use to their advantage is a charade.

Cox recognizes that, notwithstanding the issues identified above, the Court may feel compelled to address Plaintiffs' spoliation arguments. As set forth below, Cox did not have a duty to preserve transient and useless DHCP data because Cox had no clue that Plaintiffs were secretly planning this lawsuit. Rightscorp and Plaintiffs never threatened suit. Even when the lawsuit was eventually filed (*three and a half years* after Cox blacklisted Rightscorp), it was not apparent that DHCP data would matter because Plaintiffs named no "John Doe" defendants and, from the first stages of the case, Plaintiffs denied any intention to prove infringement by particular subscribers. (Even now, Plaintiffs do not intend to prove such infringement, yet the DHCP data has suddenly become "critical evidence.") In essence, Plaintiffs argue that Cox should have predicted that, despite no threat of suit, nearly four years in the future unknown entities would sue Cox for copyright infringement and those hypothetical plaintiffs would demand DHCP data that is useless in isolation. That theory collapses under its own weight.

So what is Plaintiffs' motion really about? The truth comes at the very end of Plaintiffs' brief. Before any discovery occurred in this case, Plaintiffs retained a mathematician, Robert Bardwell, to create a statistical model purportedly showing that he could attribute groups of infringements that Rightscorp allegedly observed on the Cox network to the same individuals.

Long after Plaintiffs learned that Cox had DHCP logs going back at least to the start of this lawsuit, Mr. Bardwell (whose work has been excluded and discredited by several other courts) issued a deeply flawed expert report expounding his statistical model. A month later he filed his reply report, still relying on junk statistics and false assumptions. Knowing that Cox will attack Mr. Bardwell's opinions as incompetent and untrustworthy, Plaintiffs now complain that his analysis would have been entirely unnecessary had Cox only retained more DHCP data. Plaintiffs also mislead the Court by claiming they retained Mr. Bardwell *in response to* the lack of DHCP logs, which is flatly false. Plaintiffs never moved to compel production of the DHCP logs to facilitate Mr. Bardwell's analysis. Moreover, Plaintiffs are transparently attempting to avoid the consequence of their own spoliation of the Rightscorp software that generated all the data on which Mr. Bardwell's analysis relies. This motion is a pretextual bid to gird Mr. Bardwell's flawed analysis from an inevitable and powerful *Daubert* challenge.

Even if Plaintiffs were entitled to spoliation sanctions, any remedy would have to be both related and proportional to the evidence that is no longer available. At the very most, the DHCP logs connect a particular Cox account to a particular IP address on a particular date. Those logs say nothing at all about what activity occurred at that IP address, or who was responsible for any such activity. But Plaintiffs seek an inference that they have *proved infringements* by Cox subscribers or, bolder yet, an order establishing as true *all* of Mr. Bardwell's wrong-headed conclusions regarding copyright infringement on the Cox network. Plaintiffs' request for remedies is overreaching, unfair, and legally baseless.

ARGUMENT

The Court is now well-versed in the spoliation standards in this circuit. "To establish a claim of spoliation, a movant must show that the adverse party had a duty to preserve the

allegedly spoiled documents and that the documents were intentionally destroyed." *Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 286 (E.D. Va. 2001). The Court need not reach the spoliation question here because Plaintiffs' motion is fatally defective for other reasons. But, nevertheless, Cox is not guilty of spoliation.

I. PLAINTIFFS NEVER ASKED FOR THE DHCP LOGS IN DISCOVERY.

Plaintiffs rely on invective and snark to distract attention from the fact that the motion urges severe sanctions for alleged spoliation of evidence that Plaintiffs never bothered to ask for in discovery. Conspicuously absent from Plaintiffs' brief is *any* reference to Plaintiffs' requests for production or any document request to which Cox has failed to respond. That is so because none of Plaintiffs' production requests encompass the DHCP logs.

Plaintiffs have been aware of the DHCP logs, and the role of the DHCP data in the CATS ticketing process, since March 13, 2015. On that date, Cox made its first production of documents in this case, comprising seven versions of Cox's "Residential Abuse Ticket Handling Procedures." Each of those documents described Cox's procedures (at different points in time) for dealing with complaints of alleged copyright infringement, and each stated: [redacted][1] This was a small initial production and the copyright policies specifically were obviously of keen interest to Plaintiffs, so it is inconceivable they did not review these documents. Thus, a full *five months* before the discovery cut-off of August 14, 2015, Plaintiffs were aware of the DHCP records.

[1] *See* Summary Judgment Declaration of Jason Zabek (Dkt. 321), Ex. 1 ("Residential Abuse Ticket Handling Procedures" document) at 10 (emphasis added).

Until now, Plaintiffs' focus was never on the DHCP logs but instead on subscriber PII. Plaintiffs' Interrogatory No. 13 asked Cox, in relevant part, to "[i]dentify with particularity each of Your Customers, including but not limited to by name, address, account number, the bandwidth speed associated with each account, and associated IP address(es) of each such Customer, for which You have received a DMCA Notice from Rightscorp, Inc." On April 6, 2015, Cox responded that it lacked information responsive to Interrogatory No. 13 because it never received DMCA notices from Rightscorp; but Cox also objected to the interrogatory on a number of grounds, including that it improperly invaded the privacy of Cox subscribers. For those reasons, at that time Cox did not disclose any subscriber PII to Plaintiffs.

On May 8, 2015, Plaintiffs filed a motion to compel Cox to disclose PII for subscribers associated with IP addresses at which Plaintiffs claim to have identified infringing activity. *See* Dkt. 72 (corrected memorandum). Plaintiffs sought PII for a sampling of 500 IP addresses (half from the six months before the lawsuit was filed and half from after) and also sought a "blank check" order allowing Plaintiffs to seek PII for all ***150,000*** Cox subscribers that Rightscorp's notices allegedly implicated. Plaintiffs' purported need for that information was pointedly *not* in order to prove direct infringement by any particular Cox subscriber. In the May 15, 2015 hearing on Plaintiffs' motion, the Court challenged Plaintiffs' counsel on that point:

> THE COURT: Well, what they're saying is you're saying [the PII is] not relevant. You're saying, we don't have to prove direct infringement. So why is it relevant to any claim that you are making in this case?
>
> MR. CARACAPPA: Then I may have misspoke. We – ***it's not required for us to prove direct infringement***.

Dkt. 80 at 24:1-6 (emphasis added). In the current motion, Plaintiffs reiterate that they are not seeking subscriber PII, or the DHCP data, in order to prove direct infringement by any Cox

subscriber. *See* Dkt. 340 at 8 n.3 ("Plaintiffs do not agree with Cox that the identification of individual subscribers is necessary to prove direct infringement.").

Cox opposed Plaintiffs' motion to compel subscriber PII on many grounds, including that the data was, at best, of marginal relevance in light of Plaintiffs' disclaimer of any intention to use it to prove direct infringement. *See* Dkt. 74. On May 15, 2015, the Court largely denied Plaintiffs' motion. Expressing skepticism about the broad relevance of subscriber PII in this case,[2] the Court denied Plaintiffs' request for PII associated with the 250 post-filing IP addresses and denied Plaintiffs' bid for a "blank check" to discover additional PII in the future. The Court ordered Cox to produce only subscriber PII associated with the "sampling" of 250 pre-filing IP addresses identified by Plaintiffs.

On June 5, 2015, Cox informed Plaintiffs that Cox was able to identify PII for subscribers historically associated with 139 of the 250 IP addresses identified by Plaintiffs. On that date, Cox produced PII for 122 of those historical subscribers; Cox withheld PII for the remaining 17 subscribers because those individuals contacted Cox to object to production of their private information. On June 12, 2015, Cox filed a motion for further instructions regarding how to address PII for those 17 objecting subscribers. *See* Dkt. 86. On June 23, Plaintiffs responded to Cox's motion and complained about Cox's inability to identify PII for all 250 subscribers in Plaintiffs' historical "sampling." *See* Dkt. 101 (corrected memorandum). In that brief, Plaintiffs suggested that Cox had spoliated evidence (because it could not identify some subscriber PII) and requested an "adverse evidentiary inference that prevents Cox from challenging any direct infringement proofs with respect to all the information that it has destroyed." *Id.*

---

[2] The Court observed: "And, you know, it's clear that no one is going to be involved with 150,000 customers. The case couldn't stand on that. And so, looking at a sampling with 250 is a significant sampling …." Dkt. 80 at 32:22-25.

On June 25, 2015, Cox responded and, in part, addressed Plaintiffs' spoliation accusations. *See* Dkt. 107. That brief stated that "Cox only retains DHCP logs for six months" and explained precisely why. *Id*. at 5-7. (The reasons Cox has not historically retained transient DHCP records for extended periods are discussed further below in response to Plaintiffs' renewed spoliation arguments.) The hearing on Cox's motion took place on June 26, 2015. The Court did not find that Cox spoliated any evidence and did not order any sanctions against Cox.

To summarize, as of June 26, not only were Plaintiffs fully aware that Cox utilized DHCP records to connect particular subscriber accounts to particular IP addresses and that Cox retained the data for only six months, but Plaintiffs also had specifically accused Cox of spoliation of the data. Four days later, on June 30, 2015, Plaintiffs served new discovery requests. Plaintiffs' new Request for Production No. 118 sought "[a]ll documents, since January 1, 2010, concerning or constituting your policies, procedures, and/or practices for retention or preservation of DHCP and IP address information, including records of IP addresses assigned to high speed internet subscriber accounts and DHCP lease records." Notably, ***Plaintiffs did not request the DHCP logs themselves***.

This is not the first time Plaintiffs have pursued remedies for Cox's failure to produce information that Plaintiffs never sought in discovery. On July 31, 2015, Plaintiffs filed a motion to compel Cox to produce all of the "tickets" in the CATS database. *See* Dkt. 176. At the hearing on August 7, 2015, the Court denied Plaintiffs' motion to compel in large part because none of Plaintiffs' requests for production encompassed the CATS tickets.

Perhaps recognizing the huge procedural hole in the center of this motion, Plaintiffs claim that they "moved the court in May 2015 to compel Cox to produce DHCP log data, and the Court's recognition of the importance of this data is evident in granting that motion." Dkt. 340

at 9. That statement is plainly false. Plaintiffs' motion to compel (Dkt. 72) had nothing to do with DHCP records (or any documents for that matter); that motion sought Cox subscriber PII in response to Plaintiffs' Interrogatory No. 13. And the Court largely *denied* Plaintiffs' motion. The Court allowed Plaintiffs only a "sampling" of PII associated with 250 historical IP addresses. Plaintiffs received that sampling (for a majority of the IP addresses at issue) and, as Cox discusses further below, they made virtually *no* use of the subscriber PII that Cox produced.

Spoliation occurs where a party fails "to preserve potential evidence ***for another's use*** in pending or future litigation." *Trigon*, 204 F.R.D. at 284 (emphasis added). By definition, a party cannot "spoliate" evidence that the other party has no intention or ability to use in the litigation. Stated differently, a party cannot "spoliate" information that is not evidence. Here, the DHCP logs are not evidence in this case because Plaintiffs never sought production of those logs. Consequently, Plaintiffs' motion is dead on arrival.

II. THE DHCP LOGS ARE USELESS TO PLAINTIFFS.

Even if Plaintiffs had sought production of the DHCP logs and Cox had produced those records, the data would be literally useless to Plaintiffs. That is so because the logs have no utility in isolation; they are a means for potentially connecting the dots between an IP address and a subscriber's PII. Plaintiffs already made their bid for widespread access to Cox subscribers' PII and failed. Even if Cox were to produce today every DHCP record Cox ever generated, Plaintiffs could do nothing with that information.

DHCP refers to "dynamic host configuration protocol," which is a network protocol that enables a server automatically to assign to a computer an IP address from a defined range of numbers. *See* Declaration of Brent Beck (filed in support of this brief), ¶¶ 3-4. DHCP logs allow Cox to associate a particular IP address, at a particular date and time, with a particular

cable modem media access control (MAC) address. *Id.*, ¶¶ 13-14. The MAC address is associated with a specific physical cable modem, and Cox may then be able to identify the subscriber assigned that modem at a particular time. *Id.* To make that connection between the MAC address and a particular account holder, either the CATS system or a Cox representative must compare DHCP data to customer account information (called ICOMS ID data) in a separate database. *See id.*[3] In other words, the DHCP logs do not identify subscribers; those records are just one link in the potential chain between an IP address and an account holder.[4]

Plaintiffs seize on a statement from Cox's June 2015 reply in support of its motion for instructions (Dkt. 107), that "the DHCP logs are the most direct method to connect a particular IP address with a particular subscriber at a particular date and time." That statement is true as far as it goes. The DHCP logs are a necessary *but not sufficient* component of the most direct method for connecting an IP address and a subscriber account. But, again, additional steps and other records are necessary actually to *make* that connection. The logs themselves (*i.e.*, the only evidence that Cox allegedly "spoliated") are not independently useful.

Plaintiffs' habitual lack of candor to the Court in this case is stunning. Plaintiffs claim that Cox "admits" that it did "nothing to preserve the identity of the customers with whose account each IP address was associated at the time of the infringement as identified in the [Rightscorp] infringement notices." *See* Dkt. 340 at 2, 5. Plaintiffs purport to be quoting Cox's

---

[3] The DHCP logs do not allow Cox to identify account holders with complete accuracy, because dynamic IP addresses may still be reassigned more quickly than aggregated DHCP logs will reflect. Beck Dec., ¶ 9 n.1. In other words, some IP addresses are reassigned so quickly that the logs cannot "keep up."

[4] Mr. Beck also explains in detail how the DHCP protocol functions and how Cox collects, stores, and uses DHCP data. Beck Dec., ¶¶ 4-12. It is a complex system involving over a hundred servers around the country. *Id.*, ¶ 8. Contrary to Plaintiffs' suggestions, it is not straightforward to simply retain "DHCP records."

supplemental response to Plaintiffs' Interrogatory No. 3, attached as Exhibit 22 to the Roberts Declaration (Dkt. 341), but they deliberately *alter the quote*. *See* Dkt. 340 at 5. Cox's *actual* statement, which was part of an extended discussion of Cox's processes for using and retaining DHCP records and other data, was: "As noted above, after March 14, 2011, Cox did not accept or retain Rightscorp's notices. Consequently, Cox did nothing to preserve **'**the identity of the customers with whose account each IP address was associated at the time of the infringement as identified in the Infringement Notices.**'**" (Dkt. 341), Ex. 22 at 10. Cox was simply refusing to adopt Plaintiffs' self-serving phrase quoted within Cox's response (which Plaintiffs obscure by removing the quotation marks and de-capitalizing "Infringement Notices"). Cox's response went on to note that "[i]t is possible for Cox to connect some historical account holders to particular IP addresses at particular times in the past using dynamic host configuration protocol (DHCP) records or records (if any) stored in CATS with respect to that IP address. ***CATS records are never deleted***." *Id*. (emphasis added). In fact, Cox relied on CATS records to identify PII for the 139 historical subscribers associated with the IP address "sampling" Plaintiffs identified.

Plaintiffs argue that it is "undisputed that Cox systematically destroys the ***only*** evidence identifying the direct infringing subscriber by name." Dkt. 340 at 2. That is wrong. As noted, Cox retains its CATS records, which record IP addresses and account information. By contrast, the DHCP records do not identify subscribers by name or even (standing alone) connect subscribers to IP addresses. It is possible that Plaintiffs' false claims are a result of their genuine confusion regarding DHCP data and how it functions, even though Cox has repeatedly explained it and Plaintiffs have had months to figure it out. It is equally plausible that Plaintiffs' "confusion" is pretextual and just another facet of their sleight-of-hand here. Plaintiffs do not in fact want DHCP records and could not make use of those records if they obtained them.

The DHCP records are just one means to identify subscriber PII, but Plaintiffs know that ship has sailed in this case. Instead, Plaintiffs have concocted a "gotcha" with respect to "spoliated" data and hope to bootstrap that "gotcha" into unrelated evidentiary sanctions to which Plaintiffs are not even conceivably entitled (as Cox discusses in Section IV below).

Because Cox's alleged spoliation of useless DHCP data and Plaintiffs' true motivations are unrelated to one another, Plaintiffs' motion is a mess of contradictions. As Cox noted above, Plaintiffs have consistently disclaimed any intention to prove direct infringement by any Cox subscriber, and continue to deny that such proof is necessary to Plaintiffs' claims. The Court also observed that such proof is not feasible and, consequently, denied Plaintiffs' bid to obtain widespread PII for Cox subscribers. Yet, in this motion, Plaintiffs decry Cox's purging of its stale DHCP logs because "this evidence is the only means for Plaintiffs ***to identify the Cox subscribers who have infringed their copyrights***." Dkt. 340 at 7-8 (emphasis added). Similarly, Plaintiffs lament that Cox has "stymied Plaintiffs' attempts ***to identify with specificity the individual infringers***." *Id*. at 9 (emphasis added). These disingenuous cries of prejudice eventually reach a fever pitch: "Because of Cox's deletion of relevant subscriber records linking individual subscribers to IP addresses, Plaintiffs do not have the evidence necessary ***to identify every Cox subscriber who has infringed their copyrights or exactly how many individual infringers have been using Cox's system during the relevant timeframe***." *Id*. at 13. But Plaintiffs have *never* expressed any intention to "identify individual infringers" in this case; to the contrary, Plaintiffs have consistently and vehemently *disclaimed* any such intent.

And, as is so often the case, the proof of the pudding is in the eating. In May, Plaintiffs took their shot at obtaining Cox subscriber PII. The Court granted them only a "sampling" of 250 IP addresses at which Rightscorp supposedly identified instances of alleged infringement in

the six months prior to the filing of the lawsuit. Cox produced PII for historical subscribers associated with a majority (139) of those IP addresses. And with that information — which, reading Plaintiffs' current motion, one would conclude is a crucial linchpin to their claims — Plaintiffs did … *nothing*. From those 139 subscribers, Plaintiffs managed to negotiate a settlement with just *one* individual, immunizing him from liability if he agreed to provide a declaration. That declaration did not establish that the account holder was even a Cox Internet user when he reproduced the works at issue, and the declarant [redacted][5] Those statements do not help Plaintiffs' case. In short, the reality that Plaintiffs made essentially no use of the Cox subscriber PII they did receive in June is the final act in this charade.

The timing of this motion is also suspect, to put it mildly. Plaintiffs first accused Cox in June of spoliating the DHCP data, and asked for sanctions at that time (which the Court did not grant). Plaintiffs then waited *three full months* to file this motion, until after discovery had closed and after Cox filed its summary judgment motion. Plaintiffs imply that they were surprised and shocked to learn from Cox's summary judgment motion that Cox is "brazenly" arguing that Plaintiffs lack evidence of direct infringement by any Cox subscriber. Yet in the next breath Plaintiffs admit that "[d]espite its ongoing practice of deleting all records linking specific IP addresses to specific Cox subscribers, ***during the course of this litigation Cox has made evident its intention to use as part of its defense the absence of just this data***." Dkt. 340

[5] *See* Cox's Summary Judgment Motion (Dkt. 306) at 10; 25; *see also* Bridges Declaration (Dkt. 311), ¶ 19, Ex. 61 (copy of the declaration).

at 8 (emphasis added). As the Court is well aware, at every turn in this case Cox has highlighted that Plaintiffs have the burden of proving direct infringement and cannot carry that burden with respect to any Cox subscriber. It is hardly a surprise that that argument figures prominently in Cox's summary judgment arguments. What *is* surprising is that, despite knowing that Cox did not retain pre-suit DHCP data and that Cox would challenge Plaintiffs' ability to prove direct infringement, Plaintiffs sat on their hands for months without raising these issues.

The crux of this untimely motion is that Plaintiffs want drastic evidentiary sanctions because Cox failed to preserve DHCP data that Plaintiffs never sought in discovery, that has no independent value, and that is only a means to obtain other information (PII) that Plaintiffs (i) insist they do not need and (ii) did not actually use when they got it. Those facts are a more than sufficient basis on which to deny Plaintiffs' motion outright. But those realities also provide the backdrop for the Court's consideration of Plaintiffs' weak spoliation arguments and outlandish requests for relief.

III. COX DID NOT SPOLIATE THE DHCP LOGS.

This motion rests on Plaintiffs' accusation that Cox is guilty of spoliation with respect to its historical DHCP records. Not so. Cox routinely purges stale DHCP data because that data serves no business purpose and it poses privacy risks and concerns for Cox subscribers. Contrary to Plaintiffs' assertions, Cox had no duty to suspend those routine data deletion policies, because Cox had no idea this lawsuit was coming. Even if Cox had somehow divined this future lawsuit by these particular Plaintiffs, Cox could not have anticipated that the DHCP data would matter in such a suit.

A. Cox Routinely Purges Stale DHCP Logs that Serve No Business Purpose.

Cox collects DHCP data using over one hundred servers distributed and clustered across the country. Beck Dec., ¶ 8. Those clusters of regional servers do not store DHCP data for extended periods; they keep track only of active IP address lease information for portions of regional markets. *Id*. Cox operates a "DHCP abstraction layer" in Atlanta that periodically collects data from the regional DHCP server clusters and creates aggregate reports regarding Cox IP addresses. *Id*., ¶ 9. This is truly transient data with no longer-term business utility. In the ordinary course, Cox retains the aggregate data in the abstraction layer for only thirty days. *Id*.

Relatively "fresh" DHCP data does have some utility in addressing complaints of abuse on the Cox network. As Cox discussed above, the CATS system can, under certain circumstances, use DHCP records to connect a particular IP address to a particular modem, which can then potentially be connected, using other data, to a particular Cox account. Consequently, the Cox Customer Abuse Team created its own script to further process DHCP data from the abstraction layer. Beck Dec., ¶ 10. The data goes into aggregate monthly records, which, for a single month, typically contain tens of millions of IP address assignment records. *Id*., ¶ 11. On the first of each month, an automated script archives the DHCP records for the prior month and begins populating a new table for the current month. *Id*.

In the ordinary course of business, Cox retains at least six months of archived DHCP records. Beck Dec., ¶ 12. (As a result of certain settings in the system, there are times when more than six months of records are retained. *Id*.) There is no reasonable or compelling business reason to maintain DHCP data for longer than six months; in fact, for the purposes of processing abuse complaints, even a much shorter retention period would be appropriate. *Id*., ¶ 16. That is so because complainants (in particular copyright complainants) typically send a

complaint to abuse@cox.net within a few days of the alleged abuse incident, and very often on the same day. *Id*. For example, in the last sixty days, complainants submitted a complaint between one and two days on average after the alleged incident. *Id*. Furthermore, in the last sixty days, for copyright infringement complaints specifically, there was never a delay of more than 14 days from the alleged incident to the complaint. *Id*. Consequently, "stale" DHCP data (arguably any records more than 30 days old) is of essentially no practical use. Nevertheless, Cox conservatively retains many tens of millions of those records for six months or more.

The DHCP data is also not retained for longer periods in the ordinary course because every proper abuse complaint results in a CATS ticket, and ***the CATS records are never deleted***. Beck Dec., ¶ 15. CATS currently contains approximately 15 million tickets, which correspond to over 19 million alleged abuse complaints. *Id*.[6] Plaintiffs complain that Cox has incomplete records connecting particular IP addresses to particular Cox subscribers who Plaintiffs claim are infringers. But if Plaintiffs' agent had simply revised its extortionate notices to include just the information contemplated by the DMCA, ***there would now be a record in CATS for each of those notices***. Thus, the real reason "Plaintiffs do not have the evidence necessary to identify every Cox subscriber who has [allegedly] infringed their copyrights" is that Rightscorp refused to abandon its shake down model and operate within the letter and spirit of the DMCA.

---

[6] Plaintiffs assert that Cox "ignores" more than "95% of the infringement notices it receives through blacklisting and other means." Dkt. 340 at 1. Plaintiffs arrive at that fictional percentage by including all 22 million notices that Rightscorp has purportedly sent to Cox on Plaintiffs' behalf. There is no evidence to support that alleged figure, and the number changes every time Plaintiffs file a brief. More to the point, it is now undisputed that Rightscorp's notices do not reflect actual copyright infringements, and Rightscorp grossly inflates the volume of its notices by sending multiple (sometimes thousands) of notices related to the same observation of alleged infringement. The correct statistic to focus on is that Cox is able to process over ***95%*** of the proper abuse complaints that Cox receives in an automated fashion through CATS, which is more efficient and effective for Cox and complainants alike. It is not *Cox's* system that is broken.

Not only do stale DHCP records have no practical utility or business value for Cox, but also those records create privacy concerns. Internet subscribers are reasonably worried about the long-term storage of data that they perceive allows subscribers to be "tracked," or that might be subject to data breaches or other improper uses. Beck Dec., ¶ 17. As with all subscriber data that Cox collects and stores, Cox must weigh the business value of the data against privacy concerns and other risks. Setting aside the issues of storing hundreds of millions of records Cox will never use, Cox is understandably and legitimately sensitive to the concerns of its customers.

On May 15, 2015, when the Court entered its order largely denying Plaintiffs' motion to compel but requiring Cox to produce historical subscriber PII for a "sampling" of IP addresses, Cox suspended its ordinary-course retention policies for the DHCP logs. Consequently, Cox has DHCP logs going back at least to the beginning of this lawsuit, and some records from earlier periods. Beck Dec., ¶ 12. As noted, however, Plaintiffs never sought production of those logs.

B. Cox Had No Duty to Preserve the DHCP Logs.

There is no duty to retain data indefinitely that has no business purpose, particularly transient data like Cox's DHCP logs that become stale and useless over time. *See, e.g.*, *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004), *order clarified*, No. 00 CIV. 5141 GBDJCF, 2005 WL 1514284 (S.D.N.Y. June 24, 2005) ("[T]he data at issue here are ephemeral. … No business purpose ever dictated that they be retained, even briefly. Therefore, absent the violation of a preservation order, which is not alleged here, no sanctions are warranted."); *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627, 642 (E.D. Pa. 2007) (no duty to preserve cache files). Absent other considerations, Cox obviously had no obligation to retain massive volumes of DHCP data, which serve no business purpose and raise privacy concerns. Beck Dec., ¶¶ 16-17.

Plaintiffs argue that Cox had a duty to preserve the DHCP records, presumably in perpetuity, because (1) Cox has graduated response procedures for dealing with copyright infringement complaints and is therefore always inherently acting "in anticipation of litigation" (Dkt. 340 at 3-4); and (2) Cox knew this lawsuit was coming as a result of Rightscorp's communications in 2011. Both arguments fail.

1. *Cox's Graduated Response Procedures*

Plaintiffs argue that the only reason Cox has a Customer Abuse Team, and the only reason Cox implements a graduated response process for account holders accused of copyright infringement, is to "appear to comply with DMCA safe harbor protocol so it is available when the inevitable infringement case is filed." Dkt. 340 at 3. Nonsense. Cox's Customer Abuse Team addresses all forms of abuse on the Cox network (*e.g.*, botnets, malware, phishing scams, denial of service attacks, security breaches, spam, etc.) that threaten the security and efficiency of the Cox network, or Cox account holders' interests, or both. Cox's graduated response procedures apply to all abuse types, not just copyright infringement allegations. Cox adopted all of those procedures for business reasons, not because Cox believed it would "inevitably" be sued for copyright infringement. *See* Declaration of Randall J. Cadenhead (in support of this brief) ("Cadenhead Dec."), ¶ 16.

Cox's efforts to secure the benefits of the "safe harbor" provisions of the DMCA are not a recognition that Cox was certain to face a lawsuit. Those efforts are prophylactic, to reduce and minimize risk if a dispute ever were to arise, like buying insurance. Cadenhead Dec., ¶ 16. By Plaintiffs' thinking, merely buying D&O or general commercial liability insurance would be an admission that litigation is inevitable and would trigger a duty to preserve any conceivably relevant data or records.

More to that point, even if Cox's adoption of graduated response procedures somehow triggered a duty to preserve litigation-related evidence, Plaintiffs do not explain how Cox would have known to preserve transient DHCP data. The duty to preserve evidence "arises when the party has notice that the evidence is relevant to litigation." *Trigon*, 204 F.R.D. at 287. As discussed above, proper abuse complaints generate a CATS ticket and the CATS data is *never* deleted; that is the very best record of Cox's graduated response practices. Cox could not reasonably have anticipated that DHCP data would be relevant in some future lawsuit.[7]

2. *Rightscorp's and Plaintiffs' Communications*

Next Plaintiffs argue that Cox "expected to face this litigation" because of Cox's early interactions with Rightscorp. False. In June 2011, Rightscorp's CEO, Christopher Sabec, and Cox's in-house privacy counsel, Randy Cadenhead, had an email exchange regarding Rightscorp's business. *See* Summary Judgment Declaration of Randall J. Cadenhead (Dkt. 320), Ex. 5. Far from threatening a lawsuit, Mr. Sabec was soliciting Cox to cooperate in forwarding Rightscorp's threatening "shakedown" notices to Cox subscribers and to help Rightscorp profit from extortionate settlements with Cox subscribers. Mr. Sabec candidly acknowledged that Cox had no legal obligation to forward such notices. He did not identify a plan to file a lawsuit, a rightsholder who might sue Cox, a protected work that might be at issue, or a purported specific subscriber who might have infringed. In fact, in that exchange Mr. Sabec stated: "We have zero interest in requiring Cox to terminate anyone, and ***we have zero interest in suing anyone***." *Id*.

---

[7] Plaintiffs compare this case to *Vodusek v. Bayliner Marine Corp.*, 71 F.3d 148, 156 (4th Cir. 1995), where the *plaintiff*, in the process of actively preparing to sue Bayliner for product defects, destroyed portions of the boat at issue. Dkt. 340 at 11 n.4. That holding is similar to Rightscorp's spoliation of software evidence on which it sought to build Plaintiffs' case, but it has no bearing on Plaintiffs' accusations against Cox, where Cox merely took ordinary prophylactic measures for business, rather than litigation, reasons.

(emphasis added). Mr. Sabec did not suggest an intention to take, or a timeline for taking, *any* action, let alone filing suit. *Id*. Indeed, at that time, Plaintiffs had not even retained Rightscorp.

After the initial communications in 2011 regarding Cox's decision to blacklist Rightscorp, neither Rightscorp nor Plaintiffs took any litigation-oriented action toward Cox for over *three and a half years*. Cox would occasionally receive a message from Rightscorp or Plaintiffs, but not threatening suit. For example, in November and December 2013 (a year before this lawsuit was filed), Rightscorp's CEO, Christopher Sabec, using Plaintiffs' return email addresses, emailed Mr. Cadenhead and reminded him of Cox's "obligation pursuant to 17 U.S.C. § 512(i)(1)(a) to adopt, reasonably implement, and inform your subscribers of" a repeat infringer termination policy. Of course, § 512's "safe harbor" provisions do not impose any "obligations" at all on ISPs. ISPs may, if they choose, implement procedures to avail themselves of "safe harbor" protections but there is no "obligation" to do so. More to the point, Mr. Cadenhead did not need any "reminder" of the "safe harbor" provisions because Cox already had robust graduated response procedures and a repeat infringer termination policy, which it applied reasonably. *See* Cadenhead Dec., ¶ 13. Finally, and most importantly for these purposes, those communications from Rightscorp and Plaintiffs never threatened a lawsuit.

We know now why Rightscorp and Plaintiffs were careful never to threaten litigation against Cox. Rightscorp and BMG secretly had been preparing to sue Cox since at least March 2013 (when Steptoe retained a code expert to assess Rightscorp's recordkeeping and audit procedures). But Rightscorp, the mastermind of this litigation, feared that "if Cox gets wind of the lawsuit they will immediately march into court in Atlanta (their home turf) and sue for declaratory judgement [sic]." *See* Cox's Spoliation Motion (Dkt. 255) at 8. In 2014, Rightscorp's Mr. Sabec cautioned colleagues and consultants to keep the pending lawsuit

"low key and close to the chest," to avoid a preemptive strike by Cox. *Id*. at 9. Thus, far from putting Cox *on notice* that litigation was a possibility, Rightscorp actively worked to *prevent* Cox from learning of Rightscorp's and Plaintiffs' plans. Moreover, in opposition to Cox's spoliation motion, Plaintiffs vigorously deny that they had *any* plans to sue Cox in 2013 or even most of 2014. Yet now Plaintiffs claim that *Cox* nevertheless should have known this lawsuit was coming *and* started preserving evidence in anticipation of Plaintiffs' claims.[8]

Plaintiffs' claim that Cox had a duty, before this lawsuit was filed, to preserve evidence hinges to a large degree on Mr. Cadenhead. Plaintiffs attack Mr. Cadenhead's conclusion that Rightscorp's extortionate notices were not in the spirit of the DMCA, claiming that he "provided these statements for one reason, and one reason only - so that when Cox was sued, it could rely on this 'opinion of counsel' to defend this 'blacklisting' policy." Dkt. 340 at 5. That is flatly false. As the Court will see from Mr. Cadenhead's declaration, he was not acting from any fear, let alone expectation, that Rightscorp intended to sue. He genuinely believed (and still does) that Rightscorp's notices were improper, akin to extortion or Internet scams. Cadenhead Dec., ¶ 3. Before this lawsuit was filed, he was not aware of any planned or threatened legal action against Cox by Plaintiffs or Rightscorp, and they never demanded that Cox preserve information. *Id*., ¶¶ 4-12. To the contrary, Rightscorp's communications with Mr. Cadenhead were consistently invitations to join in, and profit from, Rightscorp's schemes. *Id*., ¶ 6. And Mr. Cadenhead was

---

[8] Plaintiffs reference various communications in 2011 and 2012 by mid-level Cox employees regarding the chances of future litigation, including with Rightscorp. Some of those emails reflect the fact that Cox's distaste for Rightscorp's tactics was real and that some employees (like Mr. Zabek) welcomed a chance to defend Cox's position. Other emails reflect the reality that large companies occasionally get sued. But none reflect *anticipation* of an *actual* lawsuit by Rightscorp, let alone by these Plaintiffs, which is what is required to trigger a duty to preserve specific evidence. *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) (duty to preserve "extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.").

not aware of Rightscorp ever having sued an ISP (it had not), and the idea of litigation based on an ISP's repeat infringer termination policy seemed "far-fetched" (it is). *Id*., ¶ 15.

Plaintiffs' basic position is that, notwithstanding Rightscorp's and Plaintiffs' efforts to conceal their plans, Cox nevertheless should have predicted that, years later, this lawsuit would be filed by these Plaintiffs and that transient DHCP data (for unknown subscribers accused of infringing unknown works) would be relevant to that hypothetical suit. That position is not supported by either logic or the law.

3. *Filing of the Lawsuit*

Even when this lawsuit was finally filed in November 2014, *three-and-a-half years* after Cox blacklisted Rightscorp, it was not apparent to Cox that the DHCP logs would be relevant. That is because Plaintiffs named no "John Doe" defendants in either their original or amended complaints and, as discussed, consistently disclaimed any intention to prove direct infringement by particular Cox subscribers. In light of Plaintiffs' strategic decision, Cox had no reason to believe it would ever be required to produce PII for individual account holders, particularly when the privacy interests of those account holders dramatically outweighs any possible probative value of the PII (as starkly borne out by Plaintiffs' utter failure to capitalize on the subscriber PII they did receive). And, respectfully, Cox still believes that the Court should not have authorized even a "sampling" of subscriber PII for folks accused, without any factual support, of being "egregious infringers."

Nevertheless, when the Court entered its May 15 order requiring Cox to produce a "sampling" of PII, Cox suspended its reasonable routine purging of the archived DHCP logs. Cox has logs extending back to the start of the lawsuit, and some records from earlier periods as well. Beck Dec., ¶ 12. But, again, Plaintiffs have never asked for that information.

IV. PLAINTIFFS SEEK UNREASONABLE, INEQUITABLE, AND DISPROPORTIONATE RELIEF.

Even assuming (contrary to fact) that Cox had a duty to preserve all historical DHCP logs, the sanctions Plaintiffs seek are grossly disproportionate and untethered to anything those logs might have shown. At most, the DHCP logs are one link in the chain between an IP address and a particular Cox account on a particular date. *See* Beck Dec., ¶ 13-14. Those logs say nothing about what activity occurred at that IP address, who performed any such activity, or whether it amounted to copyright infringements. But Plaintiffs seek far more than an instruction that would connect IP addresses to Cox accounts. Instead, Plaintiffs ask for an instruction that they have proven infringements by Cox subscribers, and an order establishing as true all of Mr. Bardwell's deeply flawed conclusions regarding alleged repeated copyright infringement by individual Cox account holders. Plaintiffs are not conceivably entitled to that relief.

Spoliation sanctions must "attempt to place the prejudiced party in the evidentiary position it would have been in but for the spoliation." *Trigon*, 204 F.R.D. at 287. In addition, the sanction for a discovery violation or spoliation must bear some relation to the harm caused by the wrongful act, and be the least severe sanction necessary to remedy that wrong. *Hathcock v. Navistar Int'l Transp. Corp.*, 53 F.3d 36, 40-41 (4th Cir. 1995); *accord Cedar Petrochemicals, Inc. v. Dongbu Hannong Chemical Co.*, Ltd., 769 F. Supp. 2d 269, 290-91 (S.D.N.Y. 2011) (movant did not suffer prejudice sufficient to justify the "drastic" sanctions of exclusion of evidence: "[A]ppropriate sanctions should be tailored according to the prejudice suffered by the party seeking sanctions.") (*internal quotation and citations omitted*). Here, Plaintiffs seek disproportionately severe sanctions without proving either a wrong or any prejudice.

Plaintiffs' proposed instructions not only are disproportionately harsh, but they would also put Plaintiffs in a *far* better position than the DHCP logs ever could have. Plaintiffs seek the

following absurd instructions: (1) "Cox may not assert that Plaintiffs cannot prove ***infringement by Cox users*** of the copyrighted works as identified in Rightscorp infringement notices on the ground that the IP addresses are not tied to ***specific infringers***," and (2) Cox may not raise "any challenge to the findings of Plaintiff's [*sic*] expert, Robert A. Bardwell, concerning the probability that ***sequences of infringement*** from a single IP address are attributable to ***a single Cox subscriber***." Doc. 340 at 14, 16 (emphases added). Neither of those proposed "remedies" makes any sense in relation to alleged spoliation of the DHCP data.

A. Plaintiffs Are Not Entitled to Any Adverse Inference.

The Court must consider Plaintiffs' "evidentiary position" if all of the historical DHCP logs had been retained. *Trigon*, 204 F.R.D. at 287. In that hypothetical world, Plaintiffs' evidentiary position would be effectively what it is now. Plaintiffs have never sought the production of any DHCP records and, consequently, Cox has not produced any (though it could have if asked). The Court granted Plaintiffs access to PII only for a "sampling" of historical Cox account holders, and Plaintiffs received that sample for 139 accounts. In the hypothetical world where Cox's DHCP logs are indefinitely retained, Plaintiffs might have received a slightly larger sample (perhaps up to 250 accounts) of Cox subscriber PII. But Plaintiffs have not even argued, let alone made any showing, that PII for 111 additional Cox subscribers would have improved Plaintiffs' "evidentiary position" in any meaningful way.[9]

[9] Plaintiffs' arguments suffer from myriad critical flaws. As discussed above, Cox could not possibly have predicted, before this lawsuit was filed, that transient DHCP data would be relevant in future litigation. When the lawsuit was filed, that relevance was still not apparent because of Plaintiffs' strategic decision not to sue "John Does." But if Cox had somehow intuited that the DHCP logs would become relevant, and had immediately stopped purging those logs on the date the suit was filed, at most Cox would have DHCP data for the six months preceding the lawsuit. Yet Plaintiffs seek an adverse inference of infringement for *every* Cox account *ever* implicated by a Rightscorp notice, going back to February 2012. Plaintiffs have not attempted to tailor their requests for relief to address the alleged spoliation.

On that same note, the Court must consider any sanction in light of the harm (if any) that Plaintiffs have suffered as a result of the alleged spoliation. There has been no conceivable harm here. Plaintiffs had access to PII for 139 Cox account holders and did essentially nothing with that information. Plaintiffs cannot demonstrate (and have not even suggested) that access to PII for a few additional accounts would make any difference whatsoever. That is particularly true given that Plaintiffs continue to disavow, even in this motion, any intention or requirement to prove actual direct infringement by any particular Cox account holder.

Plaintiffs now ask the Court to preclude Cox from rebutting Plaintiffs' claims of "infringement by Cox users." Even if the Court assumed that every accused IP address could be connected to particular Cox accounts, there is no evidence that any Cox account *holder* personally committed any infringing act, much less the "repeated" infringements that Plaintiffs allege. As Cox's summary judgment motion made clear, all Plaintiffs have in support of their direct infringement claims is data that Rightscorp generated, which merely reported certain conditions at particular IP addresses. That data shows nothing about whether an individual subscriber, or someone else with access to an IP address, engaged in particular conduct.

As Rightscorp itself admits, "[t]he biggest reason for filesharing is caused by an unsecured wireless network; *anyone in a close radius can obtain access*." Dkt. 346 at 9 (emphasis added). As courts have observed, "that a copyrighted work was illegally downloaded from a certain IP address does not necessarily mean that the owner of that IP address was the infringer." *Malibu Media, LLC v. Does 1-5*, No. 12 CIV. 2950, 2012 WL 2001968, at *1 (S.D.N.Y. June 1, 2012). Infringing activity might be by "someone in the subscriber's household, a visitor with her laptop, a neighbor, or someone parked on the street at any given moment." *VPR Internationale v. Does 1-1017*, No. 11-2068, 2011 WL 8179178, at *2 (C.D. Ill. Apr. 29,

2011). Thus, even if Plaintiffs were able to use additional DHCP data to connect a particular IP address to a particular Cox account holder, it would be illogical and improper for Plaintiffs then to gain an adverse inference that that account holder personally committed any infringing acts.

In sum, the adverse inference that Plaintiffs request would put Plaintiffs in a far better "evidentiary position" than having additional DHCP data ever could, and it bears no relationship or proportionality to the spoliation that Plaintiffs allege.

B. Plaintiffs Cannot Insulate Bardwell's Flawed Analysis from Challenge.

Even more outrageous is Plaintiffs' bid to have all of Mr. Bardwell's flawed statistical "conclusions" established as true. As an initial matter, Plaintiffs imply that they retained Mr. Bardwell *in reaction to* the fact that Cox had not retained historical DHCP records. *See* Dkt. 340 at 14. That is false. Plaintiffs retained Mr. Bardwell to perform a statistical analysis of the Rightscorp data before any discovery in this case, and long before any issues concerning the DHCP logs had arisen. *See* attached Ex. A (July 27, 2015 Bardwell Dep. excerpts) at 23:14-19. Plaintiffs' motives for misrepresenting that chronology will quickly become evident.

On June 5, 2015, Plaintiffs learned that Cox had been unable to locate PII for 111 of the 250 subscribers in Plaintiffs' "sampling." On June 19, 2015, Mr. Bardwell issued his opening report purporting to "prove," through statistical analysis of *only* the Rightscorp data, that serial observations of purported infringements are attributable to a single person (to establish the notion of a "repeat infringer"). Importantly, a significant portion of the Rightscorp "infractions" data that Mr. Bardwell relied upon was from <u>after</u> the filing of the lawsuit, a period for which Cox has DHCP records. On June 23, 2015, Plaintiffs accused Cox of spoliating the DHCP records. On July 10, Cox's expert issued a detailed rebuttal report identifying many deficiencies and inaccuracies in Mr. Bardwell's analysis. On July 24, Mr. Bardwell issued his reply report.

In it, for the first time he complained bitterly about the lack of data from Cox that would verify his theories. And Plaintiffs now claim that, if Cox had only preserved DHCP data in perpetuity, Mr. Bardwell's analysis would have been entirely unnecessary. *See* Dkt. 340 at 14.

Why is that chronology important? Plaintiffs learned in June (with two full months left in the discovery period) that Cox had DHCP data going back at least to the filing of the lawsuit. Mr. Bardwell issued his opening report on June 19, and his reply report over a month later on July 24, relying on post-filing infraction data from Rightscorp. Plaintiffs now claim that the DHCP data corresponding to those post-filing infractions is so critical that it would have rendered Mr. Bardwell's analysis entirely unnecessary. And yet, ***Plaintiffs never asked for that DHCP data***. Plaintiffs never filed a motion to compel Cox to produce the existing DHCP data in Cox's possession for Mr. Bardwell's use in his analysis. That failure is inexplicable and certainly inexcusable. And it completely undermines Plaintiffs' claim that the DHCP logs were relevant, let alone critical, to Mr. Bardwell's work.

But even if Plaintiffs had requested and received the existing post-filing DHCP logs, those logs could not possibly have saved Mr. Bardwell's doomed theories. Mr. Bardwell's assertion that there were "sequences of infringement … attributable to a single Cox subscriber" (*see* Dkt. No. 340 at 16) is pure conjecture, and access to additional DHCP logs would not change that fact. Even if Plaintiffs had more data to associate an IP address with a specific Cox account, the conclusions Mr. Bardwell makes regarding repeated conduct by *account holders* remain deeply flawed. To begin with, Mr. Bardwell purports to be a mathematician, not a legal expert, yet he makes conclusions throughout his report about "infringement," a loaded legal term about which he knows nothing. *See generally Doc*. 341-1. He admits that his definition of "infringement" refers to a mere "observation" by Rightscorp of a file that is available. Ex. A

(Bardwell Dep.) at 45:1-10. And in his deposition, he confirmed that an "observation" essentially means an entry in Rightscorp's infraction table. *Id.* Mr. Bardwell also stated that the term "repeated Infringement" refers only to "multiple records for one IP address in the Rightscorp data," which cause Rightscorp to send multiple emails. *Id.* at 46:20-47:4, 51:4-10.

In other words, Mr. Bardwell simply defines Rightscorp's observations of certain conditions at an IP address as "infringements." He admits that he has no information about any Cox subscriber actually downloading or transmitting a song. *See* Ex. A at 66:1-4. When confronted with evidence of consumers receiving Rightscorp notices where a band had offered the allegedly infringing songs for free over BitTorrent, Mr. Bardwell testified that he would still count that authorized act as an "infringement." *Id.* at 96:16-97:17. He also testified that he has no opinion as to how his unique definition of "infringement" relates to or contradicts how courts define infringement. *Id.* at 59:10-14, 72:14-73:4.

Mr. Bardwell's use of the term "sequence of infringements," like his use of "repeat infringer," is also argumentative and unsupported. *See, e.g.*, Doc. 341-1 at 6. The "repeat infringer" label does not refer to any repeated act by any Internet user, much less a Cox account holder. It is based only on "repetition in the Rightscorp data" (*see* Ex. A at 51:3-10), and would attach to an account associated with an IP address that receives multiple notices for the same song on the same day, multiple notices for the same song over a span of consecutive days, and notices for each song in a .torrent file even where the IP address maps to a peer computer that has only 10% of one song in that .torrent file.[10] *See* Ex. A at 46:16-47:4, 47:14-49:12, 50:8-25,

[10] Tellingly, Mr. Bardwell was unaware of the 10% bitfield threshold in the Rightscorp code and its implications, testifying that he understood that a peer computer must have a *full* song file on it to generate a notice for that song (rather than a small portion of a *.torrent file purportedly containing that song). *See* Ex. A at 62:9-63:25. We know, of course, that is not true and that Rightscorp's "detection" systems are dramatically less reliable than Mr. Bardwell believed.

62:9-63:25, 107:20-108:3. Indeed, the data on which Mr. Bardwell relies shows that Rightscorp sent multiple notices for the same song to the same IP address over a month-long period, and sent multiple notices for one song to one IP address on the same day. *See id*. at 128:9-129:18.

Other flaws seriously undermine Mr. Bardwell's conclusions. He did not create or supervise the creation of the code that generated his calculations and conclusions; it was created by another consultant. Ex. A at 14:16-23, 17:11-18:4. Mr. Bardwell did not bother to check the accuracy of the calculations the code performed. *Id.* Furthermore, the calculations the code performed to support Mr. Bardwell's conclusions are unreliable and untestable because he never produced a functioning version of the code (which has become a central theme in this case).

It is not hyperbole to say that Mr. Bardwell's "analysis" is junk science for hire. Courts have repeatedly excluded or otherwise discredited Mr. Bardwell for precisely these types of issues. For example, in *Coleman v. Oracle USA, Inc.*, a discrimination case, the court excluded Mr. Bardwell's opinions under Rule 702, finding that they were "not relevant to [plaintiff's] claim and are so attenuated as to preclude a reasonable inference of individual disparate treatment of [plaintiff]." *Coleman v. Oracle USA, Inc.*, CIV. 09-3472, 2011 WL 2746187, at *5 (D. Minn. July 14, 2011). The court concluded that Mr. Bardwell's reports were "more likely to confuse the jury" than assist the trier of fact, they were not reliable, and they were speculative because there was "no evidence that Bardwell ruled out alternative explanations or considered relevant … variables in reaching his conclusions." *Id.* at *5-6. Finally, the court observed that, as he does here, "Bardwell relied on assumptions to make unsupported conclusions." *Id.* at *6.

Similarly, in *Manley v. Nat'l ProSource, Inc.*, the court found that Mr. Bardwell's reports failed to comply with Rule 702 and therefore failed to create genuine issues to overcome summary judgment. *Manley v. Nat'l ProSource, Inc.*, No. CIV.A. H-11-2408, 2013 WL

3480385, at *7-8 (S.D. Tex. July 10, 2013) *aff'd sub nom. Manley v. Invesco*, 555 F. App'x 344 (5th Cir. 2014) *cert. denied*, 135 S. Ct. 335, 190 L. Ed. 2d 63 (2014). The Court found that "Bardwell's methodology contains significant flaws or omissions that render his opinions unreliable and not relevant," and he provided "no meaningful explanation of how he reached his conclusions." *Id.* at *8. Likewise, in *Werede v. Allright Holdings, Inc.*, No. CIV. A03CV01167, 2005 WL 2124553, at *5 (D. Colo. Sept. 2, 2005), the court excluded Mr. Bardwell's testimony under Rule 702, concluding that his analysis was "unreliable" and that his conclusions were "not testable." *Id.*

Those themes resonate here, because Mr. Bardwell has invented a statistical "model" resting entirely on the Rightscorp data-set of "infringements," and he again has reached conclusions without any scientific basis. Mr. Bardwell learned nothing from what should have been humbling and educational experiences in the cases cited above, concluding instead that in each case the judge "got it wrong." *See* Ex. A at 205:8-16, 208:25-209:17, 214:12-17. Plaintiffs are well aware that Mr. Bardwell will face a *Daubert* challenge in this case, and he will lose. This motion is just an attempt to avoid the inevitable and to establish the indefensible.

Going back to the touchstones for a spoliation remedy, the sanction must place the party in the same "evidentiary position" it would have enjoyed without the spoliation, and the sanction must be related and proportional to the spoliation. Notwithstanding Plaintiffs' ex post facto claims, the DHCP data had no evidentiary significance for Mr. Bardwell's analysis because neither he nor Plaintiffs ever bothered to ask for it. Indeed, Plaintiffs' discovery failure on this point is so glaring that the most logical inference is that it was deliberate. Plaintiffs came into this case knowing they could not prove hundreds of thousands of individual direct infringements and openly disavowing any plan to do so. After Mr. Bardwell developed his "model" and

reached the conclusions that Plaintiffs sought, it was not in their interests to expose Mr. Bardwell to real facts or data that would compromise those conclusions.

In any event, the "remedy" Plaintiffs now seek is ludicrous. Mr. Bardwell's reports go far beyond a conclusion that a particular IP address is connected with a particular account holder for extended periods of time, which is the most the DHCP data might show. Mr. Bardwell purports to validate, again through junk science, that Rightscorp's observations reflect actual repeat infringement on the Internet by Cox subscribers. Even if there were some plausible connection between historical DHCP data and Mr. Bardwell's theories, there is no basis for the Court to leap to wholesale acceptance of Mr. Bardwell's opinions. Plaintiffs, therefore, have offered *no* rational, reasonable, or appropriate remedy for the spoliation they claim occurred. The Court should deny Plaintiffs' motion.

CONCLUSION

There is no basis whatsoever for the Court to find Cox guilty of spoliation of its DHCP records, let alone that Plaintiffs are entitled to the overreaching sanctions they seek. Cox respectfully requests that the Court deny the motion in its entirety.

Dated: October 2, 2015

Respectfully submitted,

/s/ Craig C. Reilly
Craig C. Reilly VSB # 20942
111 Oronoco Street
Alexandria, Virginia 22314
TEL: (703) 549-5354
FAX: (703) 549-5355
E-MAIL: craig.reilly@ccreillylaw.com

Counsel for Defendants

Of Counsel for Defendants

Andrew P. Bridges (*pro hac vice*)
David L. Hayes (*pro hac vice*)
Jedediah Wakefield (*pro hac vice)*
Guinevere L. Jobson (*pro hac vice*)
Fenwick & West LLP
555 California Street, 12th Floor
San Francisco, CA 94104
Tel: (415) 875-2300
Fax: (415) 281-1350
Email: abridges@fenwick.com
gjobson@fenwick.com

Brian D. Buckley (*pro hac vice)*
Fenwick & West LLP
1191 2nd Avenue, 10th Floor
Seattle, WA 98101
Tel: (206) 389-4510
Fax: (206) 389-4511
Email: bbuckley@fenwick.com

Armen N. Nercessian (*pro hac vice*)
Ronnie Solomon (*pro hac vice*)
Ciara Mittan (*pro hac vice*)
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel: (650) 988-8500
Fax: (650) 938-5200
Email: anercessian@fenwick.com
rsolomon@fenwick.com
cmittan@fenwick.com

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2015, the foregoing was filed and served electronically by the Court's CM/ECF system upon all registered users:

/s/ Craig C. Reilly
Craig C. Reilly, Esq. (VSB # 20942)
111 Oronoco Street
Alexandria, Virginia 22314
TEL (703) 549-5354
FAX (703) 549-5355
craig.reilly@ccreillylaw.com

Counsel for Defendants